ChinaXiv合作期刊

一种基于三维模型冗余贴图的信息隐藏技术 *

任　帅[a]，王　震[a]，张　弢[b†]，徐振超[a]，贺　媛[a]，苏东旭[a]，柳雨农[b]

(长安大学 a. 信息工程学院, b. 电子与控制工程学院, 西安 710064)

摘　要：针对传统三维模型信息隐藏技术鲁棒性不强的缺点，提出了一种基于三维模型冗余贴图的信息隐藏算法。首先，对正交投影纹理映射规则进行面片贴图的可行性进行验证；其次，构造带有表面颜色属性的四元数小波变换空间并选取传输的关键信息进行加密；最后，将隐秘信息嵌入鲁棒空间后生成含密 obj 模型，贴图纹理与状态信息保存至 MTL 文件中，以 RSA 编程手段进行含密模型文件加密处理。仿真实验表明，与不含表面贴图属性的三维模型水印以及隐写方法相比，该算法在特殊渲染环境下具备较强的抗攻击能力。

关键词：信息隐藏；四元数小波变换；含密 obj 模型；MTL 文件

中图分类号：TP309.2　　doi: 10.19734/j.issn.1001-3695.2018.07.0559

Information hiding algorithm based on redundant map of 3D model

Ren Shuai[a], Wang Zhen[a], Zhang Tao[b†], Xu Zhenchao[a], He Yuan[a], Su Dongxu[a], Liu Yunong[b]

(*a. School of Information Engineering, b. School of Electronic & Control Engineering, Chang'an University, Xi'an* 710064, *China*)

Abstract: Aiming at the shortcomings of the traditional 3D model information hiding technology, a novel algorithm based on obj 3D model redundant texture is proposed. First, the feasibility of the texture mapping rule of the orthogonal projection to perform the patch map was verified. Second, the model quaternion wavelet transform space with surface color attributes was constructed, and the key information to be transmitted for encryption was selected. Last, the secret message was embedded into the robust transform space to generate the stego obj model, and the texture and state information was saved into MTL. Additionally, the encrypted model file encryption process was performed by RSA programming means. Simulation experiments show that the proposed algorithm has strong anti-attack capability in special rendering environment compared with 3D model watermarking and steganography without surface mapping properties.

Key words: information hiding; quaternion Wavelet transform; secret obj model; MTL file

chinaXiv:201812.00075v1

0　引言

实际生活应用中，信息隐藏技术较之单一的密码技术具有独特的优势。传统密码技术的特性是，关键的明文信息在传输途中即使被截获，攻击分子也难以解读。但破解了加密方法后，相关人员即可将密文重组为人们可以理解的文档形式，因此密文本身容易受到不法群体的怀疑以及解密，安全性不言而喻。信息隐藏领域的相关学者不仅利用了上述传统密码加密技术的优点，同时考虑信息被截获时，破坏者仍看不见关键隐秘消息的效果。采用信息隐藏技术可以使滥用无差别攻击的极端分子按行自抑，因为互联网中多媒体数据无处不在，使原始数据消失殆尽的极端攻击没有意义。

三维模型信息隐藏技术具备良好的不可见性与较高的容量性，提高三维模型信息隐藏的鲁棒性也成为信息安全领域研究的热点。在提高模型信息嵌入容量与加强算法鲁棒性方面，文献[1]提出一种基于深度无合成误差模型的三维合成图像的可逆信息隐藏方法。其通过综合预测误差扩展算法与直方图移位算法，并优选嵌入信息的最佳像素及其映射范围，来实现隐秘信息自适应嵌入。保证载体图像鲁棒性之余，提升了隐秘信息嵌入量。文献[2]基于特定三维模型数据的稳定性优势，提出了一种基于距离映射机制的三维点云数据盲水印算法。利用三维坐标值的奇偶性完成信息嵌入，提高了算法信息容量与抗攻击能力。文献[3]在保持算法必要鲁棒性前提下，基于三维网格的拓补特征，从数学角度利用拉普拉斯矩阵提出了可以提升隐秘信息负载容量的算法。文献[4]均衡图像与三维模型数据特性，基于能量权重设计并结合三维模型轮廓结构，将坐标顶点分类并进行修改以完成高容量信息嵌入，增强了秘密信息隐写的稳健性。文献[5]提出不以模型顶点排列顺序与拓扑结构作为特征提取指标，引入视频流思想。基于帧化采样的隐马尔可夫模型小波域，实现了具有较强鲁棒性能的三维隐藏算法。文献[6]为加强三维模型信息隐藏领域中算法抵抗几何攻击的能力，利用主元分析的理论完成必要过程操作。同时结合球面坐标转换手段构造信息嵌入空间，增强了算法的鲁棒性和容量性。

文献[3~6]虽然在一定程度上提升了算法的不可见性与容量性，但对于针对性的复杂几何攻击以及相应的三维模型拓补结构操作效果甚微，鲁棒性稍弱。本文摈弃直接在三维模型表面进行稳健空间构造的做法，综合利用三维模型的额外冗余贴图空间。选定不可逆的正交投影的纹理映射规则，将对于三维模型表面特征提取的攻击操作不作用在信息变换

收稿日期：2018-07-11；**修回日期：**2018-08-30　**基金项目：**国家自然科学基金资助项目（61702050，61402052）

作者简介：任帅（1982-），男，山西太原人，副教授，博士，主要研究方向为信息隐藏理论与模型；王震（1993-），男，硕士研究生，主要研究方向为多媒体数据检索及认证；张弢（1984-），女（通信作者），副教授，博士，主要研究方向为多载体信息隐藏技术（zt904@foxmail.com）；徐振超（1992-），男，硕士研究生，主要研究方向为信息隐藏技术；贺媛（1994-），女，硕士研究生，主要研究方向为信息隐藏技术；苏东旭（1995-），男，硕士研究生，主要研究方向为数字水印技术；柳雨农（1993-），男，硕士研究生，主要研究方向为信息隐藏技术.

ChinaXiv合作期刊

chinaXiv:201812.00075v1

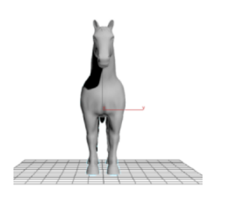
空间，增强了算法的鲁棒性。

1　信息隐藏算法步骤描述

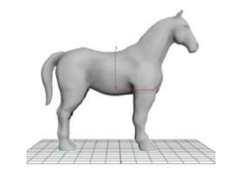
本文算法分为四个步骤：a)根据三维模型顶点及其整体拓补结构验证模型面片表面贴图的可能性，利用三维数据冗余贴图空间；b)利用四元数小波[7]变换构造待隐信息藏匿空间，并加密需要隐藏的关键信息；c)将关键秘密消息嵌入之前构造好的空间载体中；d)以非对称加密方法保留公、私钥，将含密 OBJ 文件加密传输。

1.1　OBJ 模型文件冗余数据特性与面片贴图方法

根据可携带的表面属性信息类别，三维模型有 STL、OBJ 等类型。前者不能保存贴图坐标信息，可供选择的冗余数据较少。而 OBJ 模型文件支持表面贴图渲染，并可将渲染后的场景信息如 MAX 文件加以保存，其中经渲染后的三维普通顶点、贴图顶点、法线顶点与面片信息一般保存在 MTL 文件中。算法以 War horse.stl 模型为例，展示其数据空间冗余特性，初始模型效果如图 1 所示。



(a)三维模型前视图

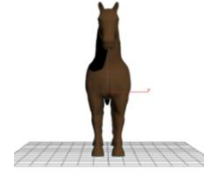


(b)三维模型左视图

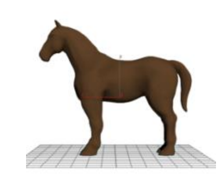
图 1　stl 格式的 Round table 模型

Fig. 1　Round table model in stl format

以 Autodesk 3Ds Max 2016 为实验平台，按内置的操作标准将初始模型更换成建筑材质的模型。从标准位图库中选取具有丰富纹理信息的未含密 Wood texture map 作为原始贴图。为提高算法抵抗攻击的能力，需选取特定的不可逆的纹理映射算法-正交投影的纹理对应规则。将木纹原始的黄色纹理信息投影在赋予建筑材质的面片表面上，冗余效果见图 2。



(a)前视图模型



(b)右视图模型

图 2　未含密三维模型

Fig. 2　Uncovered dense 3D model

综上可知，OBJ 文件具备丰富、广泛的以及可供关键隐秘信息嵌入的隐蔽空间特性。算法总体隐匿步骤如图 3 所示。

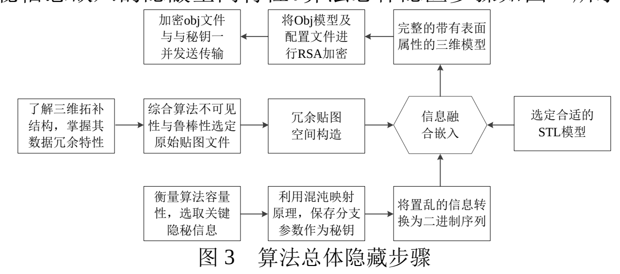


图 3　算法总体隐藏步骤

Fig. 3　Algorithm overall hidden steps

1.2　冗余贴图空间构造与关键信息加密

从标准三维模型库选取 OBJ 文件的面片贴图素材，对纹理信息较为丰富的 500×500 彩色 Wood texture map 进行冗余空间处理。为加强待隐信息嵌入空间的鲁棒性，结合四元数小波变换的正则变换特性[8]、抗几何攻击能力与平移不变形等优点。对木纹贴图素材进行四元数小波变换。须注意，信息隐匿空间的稳定性与可靠性取决于四元数滤波器[9]的分解与重构结构。本算法采用的分解结构框架具体如图 4 所示。

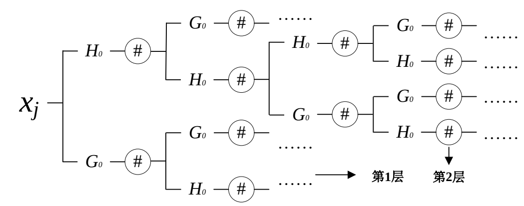


图 4　四元数小波进行分解构造框架图

Fig. 4　Quaternion wavelet decomposition structure diagram

其中，X_j 与 X_{j+1} 为四元数参数在 j 到 $j+1$ 级方向变换值的近似值。且将框架中全部的 H_0，G_0 记为四元数小波变换的低通分解与高通分解滤波器。重构框架与分解框架类似，是前者的逆过程运算。注意进行逆向运算时，之前的低通与高通分解滤波器需更换为低通与高通重构滤波器。

从数学角度分析，木纹纹理贴图 map 进行四元数小波分解后，其可表示为一个四元数解析信号。记待变换的纹理贴图为二维实信号 $g(x,y)$，其四元数解析信号 $G(x,y)$ 如式(1)所示。

$$G(x,y)=g(x,y)+g_{Hx}(x,y)i+g_{Hy}(x,y)j+g_{Hy}(x,y)k \tag{1}$$

其中：$g_{Hx}(x,y)$，$g_{Hy}(x,y)$，$g_{Hxy}(x,y)$ 分别为 Wood texture map 二维实信号 $g(x,y)$ 以 x 轴、y 轴及 x 与 y 轴的 Hilbert 变换。

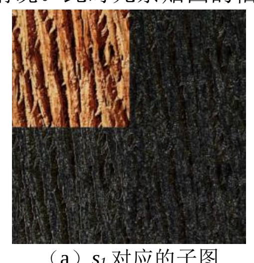
经四元小波变换后的解析信号纹理系数可转换为系数矩阵 $\boldsymbol{S}$，具体如式(2)所示。

$$S=\begin{pmatrix} LL_{\xi_h(x)\xi_h(y)} & LH_{\xi_h(x)\psi_h(y)} & HL_{\psi_h(x)\xi_h(y)} & HH_{\psi_h(x)\psi_h(y)} \\ LL_{\xi_g(x)\xi_h(y)} & LH_{\xi_g(x)\psi_h(y)} & HL_{\psi_g(x)\xi_h(y)} & HH_{\psi_g(x)\psi_h(y)} \\ LL_{\xi_h(x)\xi_g(y)} & LH_{\xi_h(x)\psi_g(y)} & HL_{\psi_h(x)\xi_g(y)} & HH_{\psi_h(x)\psi_g(y)} \\ LL_{\xi_g(x)\xi_g(y)} & LH_{\xi_g(x)\psi_g(y)} & HL_{\psi_g(x)\xi_g(y)} & HH_{\psi_g(x)\psi_g(y)} \end{pmatrix} \tag{2}$$

其中：ξ 表示图像的局部移位信息，ψ 代表图像的纹理特征，且矩阵 $\boldsymbol{S}$ 中每列对应的四元数可表示为

$$\begin{cases} s_1=LL_{\xi_h(x)\xi_h(y)}+iLH_{\xi_h(x)\psi_h(y)}+jHL_{\psi_h(x)\xi_h(y)}+kHH_{\psi_h(x)\psi_h(y)} \\ s_2=LL_{\xi_g(x)\xi_h(y)}+iLH_{\xi_g(x)\psi_h(y)}+jHL_{\psi_g(x)\xi_h(y)}+kHH_{\psi_g(x)\psi_h(y)} \\ s_3=LL_{\xi_h(x)\xi_g(y)}+iLH_{\xi_h(x)\psi_g(y)}+jHL_{\psi_h(x)\xi_g(y)}+kHH_{\psi_h(x)\psi_g(y)} \\ s_4=LL_{\xi_g(x)\xi_g(y)}+iLH_{\xi_g(x)\psi_g(y)}+jHL_{\psi_g(x)\xi_g(y)}+kHH_{\psi_g(x)\psi_g(y)} \end{cases} \tag{3}$$

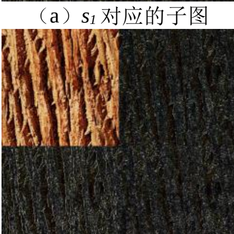
图 5(a)~(d)为经四元数小波分解滤波器变换后的纹理子图情况。此时冗余贴图的信息隐藏空间构造完成。



（a）s_1 对应的子图



（b）s_2 对应的子图



（c）s_3 对应的子图

（d）s_4 对应的子图

图 5　四元数小波变换的一级分解示意图

Fig 5 Schematic diagram of the first-order decomposition of the quaternion wavelet transform

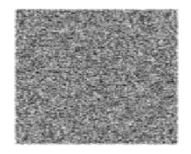
ChinaXiv合作期刊

May 提出 Logistic 映射定义，算法以 256 像素的 Chinese flag 标准方图为待隐关键信息的实验素材，利用混沌理论的预知不确定性等特征，将待隐方图的像素按非线性轨迹随机运动排列。定义式如(4)所示。

$$l(x)=\lambda x(1-x), x\in[0,1] \tag{4}$$

其中：参数 $\lambda\in[0,4]$，初始值 $x\in[0,1]$。当 $3.5699\le\lambda\le4$ 时，Chinese flag 隐秘方图即变为混沌状态。图 6 为 x =0.32，λ =4 时的实验结果状态。


(a) 原 Chinese flag


(b) 置乱后的图像


(c) 复原后的国旗

图 6　Chinese flag 混沌置乱情况

Fig. 6　Chinese flag chaotic scrambling situation

1.3　信息融合嵌入与含密表面贴图生成过程

a)考虑三维模型表面面片数量，均衡信息可嵌入容量阈值、隐秘信息保真度、关键隐秘图像传输过程中的鲁棒性。选取 500 像素的 Wood texture map 方块彩图作为 OBJ 文件的冗余数据载体，如 1.1 节所示进行四元数小波变换后构造可供隐匿的鲁棒空间。

b)将式(4)中经 Logistic 映射处理的 Chinese flag 方图置乱分支参数 λ，初始值 x 分别记为秘钥 K_1，K_2，随后转换为二进制序列 δ。

c)为保证算法良好的不可见性，且均衡后文部分采用正交投影的纹理映射规则后带有表面贴图属性的三维模型良好的实际应用效果。算法选取 1.1 节式（2）中系数矩阵 $\boldsymbol{S}$ 的高频部分，简记为 H。

d)将步骤 b)中的二进制隐秘序列 δ 融合嵌入到步骤 c)中的高频系数部分，这样满足了人眼的不可感知性。高频部分嵌入公式如式(5)所示，此时含密 Wood texture map 信息融合完成。

$$H_i'=\begin{cases} H_i+\mu\times1 & \delta_i=1 \\ H_i+\mu\times(-1) & \delta_i=0 \end{cases} \tag{5}$$

其中：H_i' 是二进制序列 δ 嵌入后的高频部分。调节信息融合嵌入程度因子 μ，可控制算法的不可见性与鲁棒性。一般 μ 越大，算法鲁棒性越强，不可见性较差；μ 越小，算法鲁棒性较弱，不可见性较好。实际应用时，可视具体场景综合考量后设置合适的信息融合因子数值。

e)将步骤 d)中 Chinese flag 序列信息融合完成后的含密 Wood texture map 按 1.1 节中的面片贴图方法进行正交投影贴图。由于选用的纹理投影算法不可逆，因此具备较强的抗攻击能力。贴图完成后带有表面颜色，亮度等属性的含密 OBJ 三维模型构造完毕。

1.4　OBJ 文件加密与传输处理

在将隐秘信息进行信道传输的实际准备阶段，需考虑传输信道的安全性与数据损坏性。OBJ 文件虽具备丰富的，可供隐秘的数据冗余空间，提高了算法的鲁棒性与不可见性，但大量分散且相异的融冗余数据也具有一定的安全性隐患。此阶段对于在隐匿空间“隐蔽”极好的含密信息，能否安全可靠的发送及尽量保持数据完善性的前提下到达接收者手中至关重要。

本文采用非对称加密方法来保证相异分散的贴图文件、MTL 纹理等信息配置文件、OBJ 模型展现状态文件等在传输与接收过程中的安全性。选定较典型的非对称 RSA 加密手段，并利用特定的 Open SS 平台命令生成 2×512 位的高保障性秘钥，关键命令如下：

Command 1：openssl genrsa -out private.key 1024。此命令用于生成接收者在后来传输过来的文件的 2×512 位解密提取码的。这是含密模型文件接收人员需提取的第一道密码私钥指令。

Command 2：openssl rsa -in private.key -pubout -out pub.key。此命令用以生成发送者发送隐秘信息之前，必须由文件接收者发送的与 Command 1 命令匹配的公钥指令。这是隐秘消息发送人员需掌握的第一道密码公钥指令。

消息发送人员利用上述第一道公钥指令，将 1.2 节中经混沌置乱转换为二值序列且完成信息融合的完整含密 obj 文件（包含贴图文件，MTL 文件，obj 模型状态文件）进行最终加密。随后将此加密 OBJ 文件与 1.3 节中秘钥 K_1，K_2（第二道密码指令）一并传输。接收人员收到文件后，利用第一道密码私钥指令进行解密，得到分散的 OBJ 模型文件后，将含密纹理贴图进行算法逆运算后，最后利用第二道秘钥指令即可提取出关键 Chinese flag 隐秘图像消息。

2　仿真实验与对比分析

采用信息隐藏技术的优点毋庸置疑，针对信息隐藏领域的攻击也层出不穷。随着网络与先进数据处理技术的发展。不法分子通常将数据进行窜改或者非严重逆损修改操作后再次进行传输，现今采用一般的信息隐藏技术，含密载体数据经历上述修改操作后，隐藏其中的关键信息大都破坏严重。

文章重点测试新算法的不可见性与鲁棒性。实验环境为 Autodesk 3Ds Max 2016，MATLAB，MeshLab，VC++，Open SS。实验模拟含密 OBJ 文件在传输过程中被截获后的模型载体状态。攻击者截获 OBJ 模型文件后，破解后可以展现的文件类型如下图 7 所示。


（a）含密贴图


（b）赋予建筑材质模型

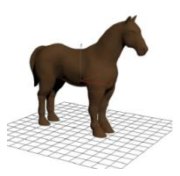

（c）含密木马模型

图 7　含密木纹贴图、备用模型与含密木马模型

Fig. 7　Contains dense grain map, alternate model and dense Trojan model

图 7(a)为含密贴图文件，经上述 1.3 节信息融合嵌入后的生成的含密木纹贴图。图 7(b)为赋予建筑材质的备用木马模型。其纹理坐标信息保存在 MTL1 文件中。图 7(c)为经正交投影的含密木马模型。

攻击者得到这些文件后首先会检测是否有可疑的消息显现。即模拟算法嵌入隐秘信息后的不可见性。

2.1　不可见性实验

根据人眼不可感知性，观察者对物体局部细节的变化或微小改动不易察觉。本文实际将隐秘二值序列隐匿到四元数信号的高频系数处，经置乱加密等处理的隐秘 Chinese flag 最终信息融合到木纹贴图的纹理边缘阴影处。

考虑最糟糕的情况，若攻击者具备深厚的专业知识素养，即使针对性的以专业图像展示软件以及 Autodesk 3Ds Max 2016 三维模型平台检测含密模型的细节边缘处，载体数据嵌入信息前后几乎没有差别，用肉眼几乎难以辨清两者的异同之处，况且截获文件里没有可供对比的原始数据载体样本。算法透明性对比实验如图 8 所示。

chinaXiv:201812.00075v1

ChinaXiv合作期刊

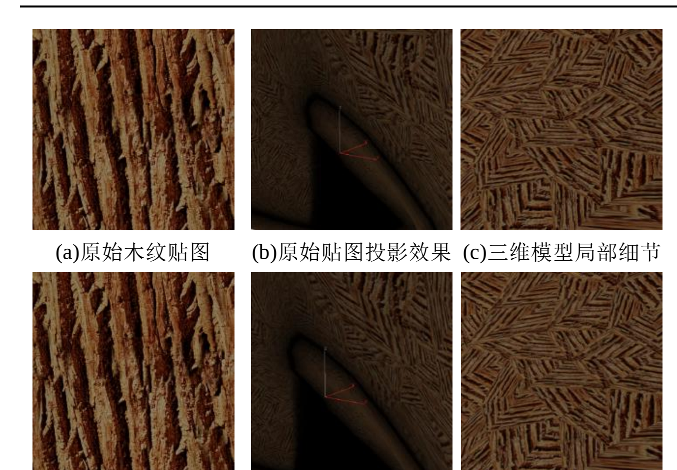


图 8　算法不可见性（透明性）实验结果

Fig. 8　Algorithm invisibility (transparency) experimental results

上述满足人眼不可见性感官对比实验较为主观。算法同时采用表述算法透明性的客观指标，利用 Metro 工具对 War horse 模型嵌入隐秘消息 Chinese flag 后的 Hausdorff 距离进行检测，隐秘消息 Chinese flag 置乱后转换的二进制总量为 $2^{17.4279}$ bit，而其 Hausdorff 距离只有 0.005162。

从载体素材类型、算法处理过程以及隐秘特征提取等方面考量，将新近文献[10,11]作为文中算法透明性的对照文献。图 9 是以客观 Hausdorff 距离指标进行参数衡量的详细统计情况。

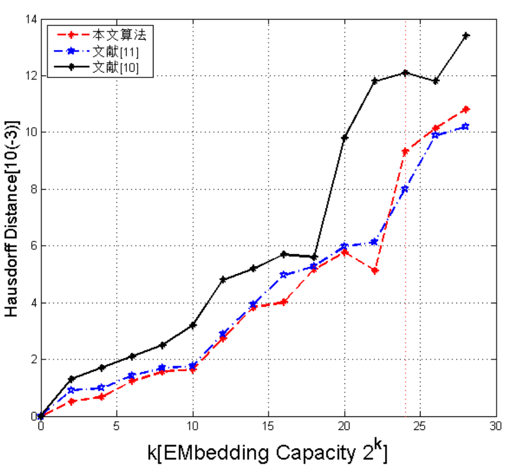


图 9　基于 Hausdorff 距离的不可见性对照实验情况

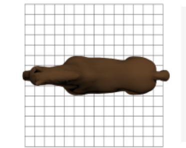
Fig. 9　Comparison of experimental results based on Hausdorff distance invisibility

其中横轴坐标表示嵌入的关键信息数据量，纵坐标为 Hausdorff 距离参数。数据嵌入强度区间 $k\in[11,23]$时，本算法的距离指标比文献[10,11]的 Hausdorff[12]距离明显小得多，因此不可见性更好；而 $k\geq 24$ 时，即当融合的关键隐秘消息总量大于 2^{24} bit 时，原纹理贴图与含密纹理贴图在细节边缘处就会发生人眼可察觉的变化。因此本算法适用于基于相异载体类型，冗余数据较分散的载体空间变换。

2.2　鲁棒性实验

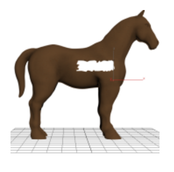
实验模拟含密 OBJ 文件在传输过程中被截获后，进行特殊攻击与窜改后算法抵抗攻击的能力。

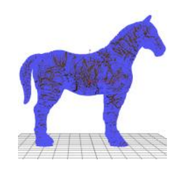
依次对目标较为明显的含密木马模型进行俯视旋转、面片挤出、面片剪切、三维顶点蓝色绘制攻击。此四类攻击利用主流专业的三维模型处理平台 Auto desk 3Ds Max 2016 进行攻击。如图 10(a)~(d)所示，仿真实验表明，经历此四种信息窜改攻击渲染后，隐秘国旗信息仍可有效提取识别。同时在不显示表明贴图属性的 MeshLab 平台对三维模型对木马模型施加噪点攻击、进行面片剔除后进行线框渲染攻击。如图 10(e)(f)所示，即使木马模型表面甚至拓补结构都已窜改变换，隐秘国旗信息仍可正常提取，信息辨识度极高。本质在于本文采用不可逆的正交投影的纹理映射算法。



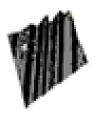



(a)旋转攻击与提取的隐秘信息　(b)面片挤出攻击与提取的隐秘信息






(c)剪切攻击与提取的隐秘信息　(d)顶点绘制攻击与提取的隐秘信息



(e)噪声攻击(meshlab 平台)　(f)按面贴图进行线框渲染攻击

图 10　特殊攻击及信息提取

Fig. 10　Special Attack and Information Extraction

同理，上文为人眼主观辨识三维模型的抗攻击性，实验后续部分采用式(6)所示的客观指标 BCR，即正确信息提取率衡量文章的算法鲁棒性强弱程度。

$$BCR = \frac{\delta'}{\Theta} \tag{6}$$

其中：分子 δ' 为遭受不同类型及各程度攻击依然可正确提取的二进制隐秘信息序列，分母 Θ 为木纹贴图载体嵌入秘密信息后的总信息位值。

将含密模型文件的带有表面贴图属性的 OBJ 模型进行如表 1 所示的平移旋转、面片裁剪、顶点加蓝绘制、拓补线框渲染等复杂类型攻击。本文算法提取的正确消息序列数值比均高于 60%，全部高于 BCR 最低阈值的 10.08%，整体上优于文献[10，11]的算法表现性能。

表 1　obj 模型鲁棒性实验 BCR 数值　/%

Table 1　Obj model robustness experiment BCR value　/%

模拟攻击方式	攻击条件与参数	本文	Ref.10	Ref.11
模型平移旋转	0-360°	82.91	71.29	79.02
面片定量挤出	面片数 202（25.8%）	78.11	69.56	71.82
面片裁剪剪切	按面剪切（22%）	71.79	21.22	53.17
顶点加蓝绘制	颜色渲染（39%）	62.74	21.05	23.91
0.1%随机加躁	Meshlab 实验平台	79.41	39.44	61.73
拓补线框渲染	按面贴图方式	65.30	13.02	19.91

三角面片作为三维模型的重要组成元素，针对其结构进行特定攻击的研究和实验尤为重要。算法着重对比面片定量挤出攻击在三维模型信息隐藏领域的信息提取性能。同样以文献上述文献对比组进行模型面片特定攻击类型的测试，统计结果如图 11 所示。其中，经历不同强度的仿真攻击实验，本文算法的稳定性较好，秘密信息提取率均超过 65%，受攻击环境的影响较小，鲁棒性较强。

chinaXiv:201812.00075v1

ChinaXiv合作期刊

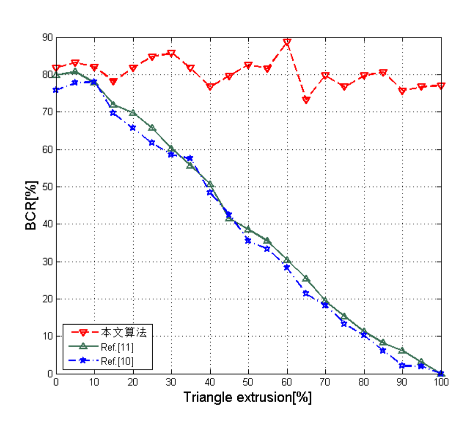


图 11 面片挤出攻击鲁棒性对此实验数据

Fig. 11 Patch extrusion attack robustness for this experimental data

在 Auto desk 3Ds Max 2016 实验攻击平台选中按面剪切的渲染模型，同时控制面片剪切的攻击，统计结果如图 12 所示。可以看出当 OBJ 模型面片剪切区域比例覆盖到达 40%时，本算法 BCR 提取率高达 80.07%，在同领域其他的研究算法显示处良好的隐秘信息复原能力，最后，在仿真攻击平台加大面片裁剪强度至 80%，归因于四元数变换[13]与相异载体特征图像融合原理，正确消息序列仍能高比率提取。

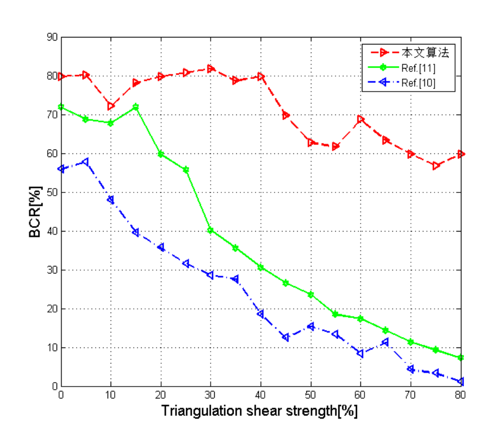


图 12 面片剪切鲁棒性对比实验

Fig. 12 Comparison of patch shear robustness

进行顶点加蓝绘制攻击，将 War horse.stl 模型顶点分别进行不同强度的绘制重排实验，对比结果如图 13 所示。模型顶点绘制重排程度接近 80%时，本文算法提取出的信息仍可以有效识别，BCR 比值均大于 60%，表明本文 obj 模型算法针对三维顶点的特定类型攻击同样具有较强的抗攻击能力。

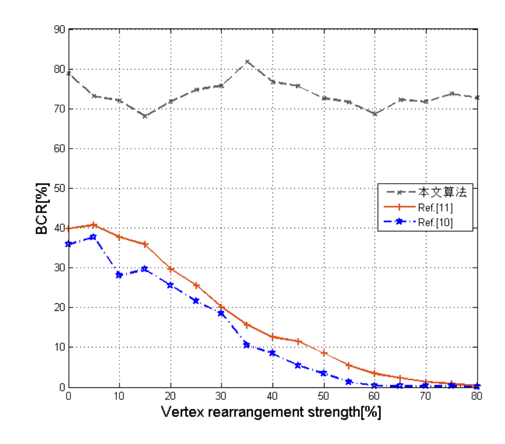


图 13 顶点绘制攻击鲁棒性对比实验

Fig. 13 Robust comparison experiment of vertex drawing attack

总结上述各类型实验统计结果，可看出本文算法适用于相异分散数据载体的信息隐藏，即多载体低密度的秘密文件隐匿，同时，针对三维模型数据组成与拓补结构特点的面片定量挤出、面片区域性裁剪、三维顶点颜色绘制等类型的攻击均具备较强的鲁棒性。最后算法良好的不可见性使该隐藏技术在特殊环境下也可广泛应用。

3 结束语

综上可知，本文基于 OBJ 模型贴图数据冗余特性，综合利用四元数小波变换、混沌映射算法以及 RSA 分对称加密手段。将隐秘消息隐秘在贴图空间中，且贴图载体仅呈现在三维模型面片表面。满足三维模型表面颜色属性可视化的基础上，保证了信息隐藏技术的性能要求。仿真实验表明，算法适用于对鲁棒性要求较高的场景应用环境。然而，算法的隐秘信息嵌入容量[14]会因 Auto desk 3Ds Max 2016 与 MeshLab 平台的功能性与时效性变化而变化，且在保持一定的算法鲁棒性后，可嵌入信息的容量会收到贴图载体空间[15]的限制。故在后续的研究当中，着重建立此类算法容量性评价体系之余，可尝试多幅贴图载体群的信息隐藏算法。

参考文献：

[1] 欧博，石向莲．基于深度无合成误差模型的三维图像可逆信息隐藏方法研究 [J]．信息网络安全, 2018(5): 24-31. (Ou Bo, Shi Xianglian. Reversible data hiding for three-dimensional image based on depth no-synthesis-error model [J]. Information Network Security, 2018(5): 24-31.)

[2] 王刚，任娜，朱长青，等．倾斜摄影三维模型数字水印算法 [J]．地球信息科学学报, 2018, 20(6): 738-743. (Wang Gang, Ren Na, Zhu Changqing, , et al. The digital watermarking algorithm for 3D models of oblique photography [J]. Journal of Geo-Information Science, 2018, 20(6): 738-743.)

[3] 李世群，李桂清，冼楚华．三维网格模型特征向量水印嵌入[J]．图学学报, 2017, 38(2): 155-161. (Li Shiqun, Li Guiqing, Xian Chuhua. Eigenvector-based watermarking for 3D Mesh models [J]. Journal Of Graphics, 2017, 38 (2): 155-161.)

[4] 雷敬祥．基于能量权重的信息隐写算法设计与研究 [D].西安：长安大学, 2016：39-48. (Lei Jingxiang. Design and research of Information Steganography Algorithm Based on energy weight [D].Xi’an: Chang’an University, 2016:39-48.)

[5] 綦科，张大方，谢冬青．基于帧化采样和小波 HMM 的三维模型信息隐藏[J]．计算机辅助设计与图形学学报, 2010, 22(8): 1406-1411. (Qi Ke, Zhang Dafang, Xie Dongqing. Steganography for three-dimensional model based on frame transform and HMM model in wavelet domain [J]. Journal of Computer-Aided Design & Computer Graphics, 2010, 22(8): 1406-1411.)

[6] 任帅，张弢，杨涛，等．基于三维模型球型分割的信息隐藏算法[J]．计算机应用, 2017, 37(9): 2576-2580. (Ren Shuai, Zhang Tao, Yang Tao, *et al.* Information hiding algorithm based on spherical segmentation of three-dimensional model[J]. Journal of Computer Application, 2017, 37(9): 2576-2580.)

[7] Soulard R, Carré P. Quaternionic wavelets for texture classification [J]. Pattern Recognition Letters, 2011, 32(13): 1669-1678.

[8] Bahri M, Ashino R. Relationship between quaternion linear canonical and quaternion fourier transforms [C]//Proc of International Conference on Wavelet Analysis and Pattern Recognition. Piscataway, NJ: IEEE Press, 2014: 116-121.

chinaXiv:201812.00075v1

ChinaXiv合作期刊

[9] 殷明. 四元数小波变换理论及其在图像处理中的应用研究[D].合肥：合肥工业大学，2012. (Yin Ming. Research on quaternion wavelet transformation theory and its application in image processing[D].Hefei: HeFei University of Technology,2012.)

[10] 王新宇，詹永照. 构造顶点分布特征的三维模型数字水印算法[J]. 计算机辅助设计与图形学学报, 2014, 26(2): 272-279. (Wang Xinyu, Zhan Yongzhao. A watermarking scheme for three-dimensional models by constructing vertex distribution characteristics [J]. Journal of Computer-Aided Design & Computer Graphics, 2014, 26(2): 272-279.)

[11] 杨飚，吕梦琪，王宜敏，等. 基于复杂区域多层嵌入的三维模型隐写[J]. 电子测量技术, 2016, 39(12): 164-167. (Yang Biao, Lyu Mengqi, Wang Yimin, *et al*. Structure complexity based multi-layer steganography for 3D model[J]. Electronic Measurement Technology, 2016, 39(12): 164-167.)

[12] Carlson N A, Porter J R. On the cardinality of Hausdorff spaces and H-closed spaces [J]. Topology & Its Applications, 2013, 160(1): 137-142.

[13] Khoubani S, Hassan M M, Sheikhhosseini M. Quaternion wavelet frame rate up-conversion [C]// Proc of the 24th National and 2nd International Iranian Conference on Biomedical Engineering. Piscataway, NJ: IEEE Press, 2017: 1-5.

[14] 韩佳伶. 基于隐藏容量的数字图像信息隐藏算法研究 [D]. 长春：吉林大学，2015： 34-42. (Han Jialing. Research on digital image information hiding algorithms based on hiding capacity [D].Changchun: Jilin University, 2015:34-42.)

[15] Chai Pengfei, Luo Xiaoqing, Zhang Zhancheng. Image fusion using quaternion wavelet transform and multiple features [J]. IEEE Access, 2017, (99): 1.

chinaXiv:201812.00075v1